

Appln No. 09/305,951
Amdt. Dated October 13, 2004
Response to Office action of August 13, 2004

2

REMARKS/ARGUMENTS

The Office Action has been carefully considered. The issues raised are respectfully submitted to be traversed and addressed below with reference to the relevant headings and paragraph numbers appearing under the Detailed Action of the Office Action.

"Claim Rejections – 35 USC § 103"

At pages 2 to 5 of the Office Action, the Examiner rejects claims 1 to 4, 6 to 15, and 17 to 20 under 35 U.S.C. §103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann *et al* US Patent 5608800.

Claim 1 of the present application describes a validation protocol for determining whether an untrusted authentication chip is valid, or not. The Applicant respectfully submits that claim 1 is not obvious over Sony in view of Hoffmann.

With respect to Sony, Sony describes a mutual authentication method, where there are two untrusted IC cards (abstract). The Examiner has asserted that Sony does not describe the calculation and comparison of a digital signature as a step of the authentication method. Additionally, in contrast to the present claim 1, the Applicant submits that Sony does not describe encrypting and decrypting data in a trusted and an untrusted authentication chip. In particular, the process described by Sony requires the use of a reader/writer to transmit the codes (see abstract), as well as encrypt the random number RA using the key KA, and comparing it to the original random number RA. Thus, as features of the present claim 1 are not described by Sony, claim 1 is patentable over Sony.

With regard to Hoffmann, Hoffmann relies on an enciphered signature obtained from a combination of coupling data and random data (abstract). The signature that is described by Hoffmann is developed from useful data and is symmetrically enciphered by a key which is derived from the coupling data designating the transmission between the transmitter and receiver (column 2, line 1 to 6). In contrast to Hoffmann, claim 1 describes generating a secret random number and calculating a signature for the random number using a signature function, whereas in Hoffmann the random data is enciphered by a transfer key and not a signature function (column 2, lines 25 to 27).

Furthermore, Hoffmann requires a message comprising the useful data, the enciphered signature, the coupling data, and the enciphered random data, as well as the transfer key to be transmitted in order to determine whether there has been an introduction of unauthorised data in the transmitted data (columns 2, figure 2). In contrast, claim 1 of the present application, describes the passing of the encrypted random number and the signature from the trusted authentication chip to an untrusted authentication chip. Thus, claim 1 has the advantage over Hoffmann in that it does not require the passing of so many different elements, in order to attain authentication.

Additionally, Hoffmann describes a process wherein once the "coupling data are checked on the receiver side" to determine whether there is a discrepancy, and if there is unauthorised data, the message is rejected (col 2). Thus, the random data "are recovered by deciphering with the transfer key the enciphered random data obtained, the symmetric key is determined by one-way enciphering of the combination of the calculated random data and coupling data obtained, the signature is recovered by deciphering the enciphered signature with the aid of

Appn No. 09/505,951
Amdt. Dated October 13, 2004
Response to Office action of August 13, 2004

3

the calculated key, the signature is checked and, if errors are established, the method is rejected" (column 2).

In contrast, claim 1 describes a validation protocol, wherein once the encrypted random number and signature are passed from the trusted authentication chip to the untrusted authentication chip, the following steps occur:

- the encrypted random number and the signature are decrypted with a symmetric decryption function, using the first key, in the untrusted authentication chip;
- a signature is calculated for the decrypted random number using the signature function, in the untrusted authentication chip;
- the signature calculated is then compared to the signature decrypted in the untrusted authentication chip;
- if the two signatures match, the decrypted random number is encrypted by the symmetric encryption function using a second key and is returned to the trusted authentication chip;
- the random number in the trusted authentication chip is encrypted by the symmetric encryption function using the second key;
- the two random numbers which have been encrypted by the second key are compared, in the trusted authentication chip;
- if the two random numbers match, then the untrusted authentication chip is valid. Otherwise, the untrusted authentication chip is invalid.

Thus, the processes described by Hoffman and claim 1 are entirely different. The Applicant respectfully submits that in establishing secure systems, these are not trivial differences. In particular, different methods of enciphering and deciphering the information relayed in security systems, even with slight differences, are imperative in order to prevent and detect possible hacking of the system.

As neither Sony nor Hoffmann teach or suggest the features of a validation protocol as described by claim 1, the present claim 1 is patentable over the cited prior art. Similar arguments also apply to claim 11.

Furthermore, there is a lack of motivation by the person skilled in the art, to combine Sony and Hoffmann. Sony is directed towards mutual authentication of IC cards (abstract), whereas Hoffmann is concerned with determining "unauthorised introduction of data" (column 1, lines 9 to 10), wherein relayed messages between a transmitter and receiver are authenticated, and is not concerned with authenticating a chip.

If, however, a person skilled in the art were to combine the teachings of Sony and Hoffmann, the present claim 1 would not be obvious in view of the combination. In particular, a combination of Sony and Hoffmann does not teach, nor suggest the features of claim 1 such as enciphering and deciphering data in a trusted and an untrusted chip, or calculating a signature for the random number by using a signature function. Thus, it is respectfully submitted that claim 1 of the present application is patentable over the cited

Appln No. 09/505,951
Amdt. Dated October 13, 2004
Response to Office action of August 13, 2004


4

prior art.

In light of the above, it is respectfully submitted that the claim rejections have been successfully traversed and addressed. Accordingly, it is respectfully submitted that the claims, and the application as a whole with these claims, are allowable, and a favourable reconsideration is therefore earnestly solicited.

Very respectfully,

Applicants:


SIMON ROBERT WAMSLEY


PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762